sumsub | CertiSur

Confianza desde el primer día

Cómo las instituciones financieras argentinas pueden reducir los casos de fraude sin ralentizar a los usuarios legítimos



Confianza digital y verificación a lo largo de todo el ciclo de vida en el mercado argentino en 2026

Resumen ejecutivo

La digitalización en Argentina ha avanzado más rápido que su infraestructura de verificación. Una población que da prioridad al uso de los teléfonos inteligentes, un mercado de pagos que crece más del 70 % interanual y 8,1 millones de personas que ahora cuentan con créditos de fintech han abierto enormes oportunidades comerciales y un terreno igualmente amplio para el fraude.

El modelo antiguo, en el que la identidad se verifica una sola vez al abrir la cuenta y se da por válida a partir de ese momento, ya no es válido. El fraude en Argentina está automatizado, cada vez más asistido por inteligencia artificial y se extiende a lo largo de todo el ciclo de vida del cliente: documentos de identidad falsificados en la primera línea de contacto, phishing a través de WhatsApp y Telegram, cuentas mula reclutadas en redes sociales y dispositivos manipulados que eluden los chequeos estáticos.

Este informe sostiene que para reducir el fraude sin penalizar a los usuarios de buena fe es necesaria una plataforma integrada que aplique medidas de control basadas en el riesgo, desde el primer día de incorporación hasta cada una de las transacciones posteriores. Descubrirá los datos del mercado local, los vectores de fraude específicos, los obstáculos de las empresas que frenan la modernización y un modelo operativo práctico de verificación que abarca todo el ciclo de vida de la cuenta.

La situación de las finanzas digitales en Argentina

Todos los servicios financieros de Argentina dependen de los teléfonos móviles. El 94 % de la población tiene un teléfono inteligente, hay 64,7 millones de líneas móviles activas frente a una población de aproximadamente 46 millones (lo que supone una penetración de alrededor del 141 %), y el 90 % de los argentinos se conecta a Internet, según el Informe sobre la percepción de la seguridad digital de Certisur. Especialmente en los segmentos de menor poder adquisitivo, un único dispositivo móvil concentra las operaciones bancarias, los pagos y el trabajo.

Ese comportamiento transformó el sistema financiero más rápido de lo que la mayoría de las instituciones habían previsto. En junio de 2024, 36,8 millones de personas tenían una cuenta, y el 73,8 % de los titulares de cuentas había registrado al menos una transacción durante el trimestre, lo que supone un aumento de 12,4 puntos porcentuales con respecto al mismo periodo del año anterior. Los pagos electrónicos superaron los 40 por adulto al mes, lo que supone un aumento del 73 % con respecto al mismo periodo del año anterior, y fueron las transferencias inmediatas las que más contribuyeron a desplazar el efectivo de la vida cotidiana.



El porcentaje de adultos que disponen tanto de una cuenta bancaria como de una cuenta de pago alcanzó el 66,4 %, y solo una cuarta parte de quienes tenían ambas cuentas se quedó con un único proveedor, lo que pone de manifiesto hasta qué punto se ha convertido en algo habitual en todo el país el uso de aplicaciones de pago interoperables.

Este mismo reflejo digital se observa en el ámbito del ahorro, donde las cuentas de pago con saldos en fondos del mercado monetario pasaron de 13,8 millones a 18,6 millones en el primer semestre de 2024, lo que supone que aproximadamente la mitad de los titulares de cuentas de pago están poniendo sus pesos ociosos en una aplicación para obtener beneficios.

La situación crediticia es donde la presión se hace más patente. El crédito al sector privado representa el 13,1 % del PBI en Argentina, frente a una media de América Latina del 47,8 % y a cifras superiores al 74 % en Chile y Brasil.





El país adolece de un déficit de crédito, y las entidades que están cubriendo esa carencia son, cada vez más, las digitales. En la actualidad, más de 8,1 millones de personas tienen un crédito de una fintech, lo que supone casi 4 de cada 10 personas con algún tipo de crédito formal, frente a los 3,7 millones de hace dos años. Las fintechs conceden uno de cada cuatro créditos activos del sistema, aunque solo representan el 3,3 % del volumen, ya que el importe medio de un préstamo de una fintech a un particular es de 541 394 ARS, frente a los más de 4,1 millones de ARS de los bancos tradicionales.

Hay dos detalles de esos datos que resultan importantes para cualquiera que diseñe flujos de verificación:

- En primer lugar, se trata de un negocio con un gran volumen, precios bajos y márgenes reducidos, por lo que cada solicitud abandonada y cada pérdida por fraude afecta gravemente a la rentabilidad unitaria.

- En segundo lugar, los nuevos prestatarios no forman parte de la base de clientes actual de las entidades tradicionales. El 53 % de los usuarios de créditos de fintech son mujeres y el 51 % tienen entre 18 y 39 años, un colectivo más joven, para el que el móvil es la prioridad, que se incorpora por primera vez al sistema financiero formal. Los usuarios que utilizan estos servicios por primera vez y los expedientes crediticios con poca información son precisamente las circunstancias en las que aumenta el riesgo de fraudes con la identidad.



Néstor Markowicz
Director General de CertiSur

"En Argentina, el principal reto consiste en mantener la confianza durante toda la relación con el cliente. Los usuarios aceptan de buen grado los procesos de validación siempre que sean sencillos, rápidos y transparentes.

Por otra parte, el aumento de los casos de fraude y de las amenazas impulsadas por la inteligencia artificial hace necesario pasar de un único chequeo en la incorporación a una verificación de identidad continua durante todo el ciclo de vida".

Por qué el modelo de única incorporación es erróneo

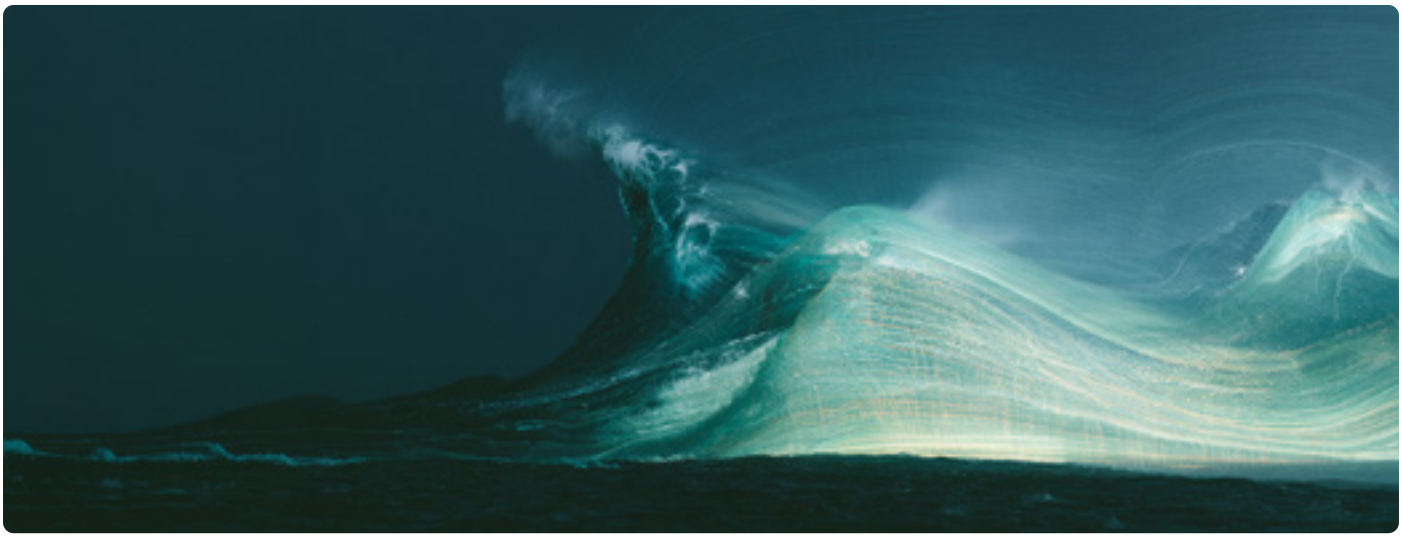
Durante años, las entidades financieras argentinas consideraban la identidad como una confirmación única que se realizaba al abrir la cuenta y en la que se confiaba a partir de ese momento. La experiencia local apunta a que el abandono se debe a una acumulación de pasos de validación, a la necesidad de subir documentos manualmente, a la exigencia de imágenes de alta calidad y a flujos que obligan a los usuarios a cambiar de canal a mitad del proceso. En Argentina no existe un indicador público consolidado sobre el abandono durante la incorporación, por lo que cualquier cifra nacional precisa no es más que una estimación. Lo que sí se observa, sin embargo, es la tendencia general: las instituciones están automatizando los controles, incorporando datos biométricos y realizando comprobaciones de antecedentes para aumentar la conversión sin descuidar la seguridad.

El problema más costoso se produce más adelante, en el vacío que se abre en cuanto finaliza la incorporación. Cuando los datos recopilados al abrir la cuenta nunca reflejan lo que el usuario hace después, la entidad se queda con una imagen estática de una persona cuyo perfil de riesgo está en constante evolución. Credenciales robadas mediante phishing, dispositivos que cambian de manos, cambios en el comportamiento... y la lista sigue. El hecho de que la incorporación se haya realizado sin problemas hace seis meses no indica en absoluto si la sesión que se está usando en este momento corresponde a la misma persona.

Este informe aboga por un cambio de perspectiva que consista en considerar la incorporación como el primer día de una relación continua, lo que coincide con la dirección que está tomando la normativa. El BCRA ha establecido una serie de obligaciones anti-fraude y ciberseguridad durante toda la cadena de pagos, y la Ley 27.739 incluyó a los proveedores de servicios de pago, los servicios de activos virtuales y los proveedores de crédito no financieros en el ámbito de aplicación como entidades obligadas a informar ante la Unidad de Inteligencia Financiera (UIF), según la guía Chambers Fintech 2026 para Argentina.

El proceso basado en el riesgo

Adaptar el nivel de verificación al riesgo de cada usuario permite mantener las trabas donde deben estar, y la verificación sin documentos demuestra cómo funciona esto en el mercado argentino. La identidad de los usuarios de bajo riesgo puede verificarse a partir de fuentes de datos locales fiables, como bases de datos gubernamentales y chequeos bancarios, sin necesidad de subir ningún documento. De este modo se elimina la principal fuente de errores manuales y abandonos. El solicitante no tiene que hacer ninguna foto y, aun así, la identidad se verifica en unos segundos.



La verificación sin documentos funciona como la vía predeterminada en un proceso basado en el riesgo, reservada para aquellos usuarios cuyos indicadores parecen lo suficientemente fiables, y en la que se introducen medidas de seguridad más estrictas en cuanto se detecta alguna anomalía. Una discrepancia en los datos, un dispositivo desconocido, una primera transacción de elevado valor o una alerta de jurisdicción dan lugar a controles más exhaustivos, como la validación de documentos y la verificación de vida con datos biométricos. La mayoría de los usuarios siguen un proceso sencillo, y los chequeos solo se intensifican para aquellos cuyas señales lo justifican.

Fijarse como objetivo la fricción cero es un error. Los estafadores se aprovechan de un proceso que no exige nada a nadie ni verifica a nadie de inmediato. El objetivo es que las restricciones no supongan un obstáculo para los usuarios que actúan correctamente y que se activen automáticamente cuando cambie el panorama de riesgo, algo que ocurre con frecuencia.

Por qué la acumulación de tecnologías anteriores fallan en este modelo

Para muchas empresas argentinas, el hecho de querer adoptar este modelo y ponerlo en práctica es una cuestión de arquitectura, y los obstáculos que Certisur detecta en los bancos locales son recurrentes.

Los plazos de desarrollo internos son lentos y escasean las API modernas que permitan conectar las nuevas herramientas con las antiguas. Las herramientas de verificación de identidad, control de fraude y autenticación no están conectadas y tienen escasa interoperabilidad, por lo que una señal detectada en un sistema nunca llega al equipo que la necesita. La revisión manual sigue siendo una carga de trabajo excesiva. Pasar de las comprobaciones puntuales a la supervisión continua requiere un modelo operativo que la mayoría de las instituciones aún no han desarrollado. Eso es lo que se podría denominar sistemas bancarios centrales rígidos, reacios a integrarse con los flujos de verificación modernos.

Cada herramienta desconectada conlleva además un costo de cumplimiento que rara vez aparece en la factura. Cuando los datos de incorporación, los datos de transacciones y las señales de fraude están en sistemas diferentes, cada auditoría, cada informe de actividad sospechosa y cada investigación se convierten en un ejercicio de conciliación manual. De forma imperceptible, se va agravando el problema y la situación empeora a medida que aumenta el volumen. El mercado ya está avanzando en la dirección contraria: el BCRA y la UIF han autorizado la incorporación totalmente digital y, en la actualidad, ya operan en Argentina bancos 100 % digitales, lo que eleva el estándar de lo que se espera de un proceso moderno.

Cómo opera el fraude hoy en Argentina

El robo de identidad mediante phishing sigue siendo la principal amenaza en Argentina, y los canales utilizados son aquellos que la gente usa a diario: WhatsApp, Telegram, el correo electrónico y las llamadas telefónicas directas.

Sin embargo, lo que cambia todo es la automatización. El phishing a gran escala asistido por IA ha convertido la suplantación de identidad en un proceso industrial: en el Informe sobre la percepción de la seguridad digital de Certisur, el 43 % de los argentinos afirmó haber sufrido un ataque informático o un fraude digital durante 2025 y el primer semestre de 2026, lo que supone un fuerte aumento con respecto al 33 % registrado antes. Esa cifra mide la percepción declarada por los propios encuestados, por lo que se interpreta mejor como un indicador de hasta qué punto las personas se sienten expuestas, lo cual tiene su propio peso comercial cuando la confianza impulsa la conversión.

Hay tres aspectos que merecen una atención especial:

1

Alteración de documentos de identidad

Los documentos nacionales de identidad (DNI) modificados y falsificados se utilizan para burlar los controles de incorporación de baja seguridad, y precisamente por eso los chequeos de documentos, combinados con la validación en bases de datos y la verificación de la presencia del titular, ofrecen mejores resultados que los chequeos de documentos por sí solos.

2

Redes de mulas (cuentas mulas)

Las cuentas mula se reclutan abiertamente: los delincuentes ofrecen dinero en efectivo en TikTok y Telegram a cambio del acceso a las cuentas. Las cuentas mulas son, por definición, un problema relacionado con el ciclo de vida: la cuenta se abre sin irregularidades y se vuelve sospechosa más adelante, por lo que pasa desapercibida para cualquier sistema de control que deje de controlarla después del primer día.

3

Manipulación de la sesión o del dispositivo

Las herramientas que ocultan la identidad real de un dispositivo, manipulan sesiones o automatizan acciones se utilizan cada vez más para eludir los chequeos iniciales, lo que traslada la carga de la detección hacia la inteligencia de dispositivos y las señales de comportamiento que los documentos por sí solos no pueden proporcionar.

Ninguno de ellos se detecta de forma fiable en un único punto de control. Las identidades falsas, el comportamiento de mulas de dinero y las sesiones manipuladas se van revelando con el tiempo y a través de diversas señales, lo que justifica la combinación de la validación de documentos, la biometría, el análisis de comportamiento y el monitoreo de transacciones en un único sistema. Las instituciones locales ya están invirtiendo en ese sentido, combinando la validación de documentos con el análisis de riesgos en tiempo real para detectar identidades falsas y movimientos ilícitos de fondos.



El modelo de plataforma única

Una defensa que se adapta al fraude distribuido integra la verificación de identidad, las señales de los dispositivos, la biometría, la detección AML y el monitoreo en una única capa compartida, en la que cada elemento aporta información a los demás. Se debería ver así:

- **Datos de incorporación** que alimentan normas de monitoreo.
- Una **huella digital del dispositivo**, del momento del registro, está disponible cuando se detecta una transacción sospechosa meses después.
- Entonces **la detección de un caso positivo** y una anomalía de comportamiento se encuentran en el mismo caso, ante el mismo analista, en lugar de en dos sistemas distintos a cargo de dos equipos diferentes.
- **El resultado es una revisión más rápida**, y esa eficiencia se nota justo donde más importa a las instituciones: en la plantilla y en los plazos de tramitación.

Aquí es donde la colaboración entre Certisur y Sumsub encaja en el mercado argentino.

Certisur aporta la infraestructura de confianza local en la que ya confían los bancos y las empresas argentinas: firmas electrónicas, certificados digitales, identidad digital y la reputación de un actor local consolidado dentro del sector regulado.

Sumsub ofrece una plataforma que unifica la verificación, la prevención del fraude y el monitoreo durante todo el recorrido del cliente, con la cobertura global y la capacidad de Travel Rule que importa, en un momento en que el volumen de criptomonedas en Argentina sigue aumentando, con más de 2,5 millones de usuarios mensuales de criptomonedas y más de 93 900 millones de dólares en transacciones en cadena durante el último año (Chambers Fintech 2026).

Esta combinación ya está dando buenos resultados en otros lugares de la región:

El Dorado, una aplicación líder en pagos entre particulares (P2P) y monedas estables que presta servicio a más de 250 000 usuarios en toda América Latina, verifica a los nuevos usuarios en una media de 18 segundos y aprueba al 99 % de ellos desde que se pasó a Sumsub en 2022. El equipo llevó a cabo la integración mediante un web SDK en cuestión de días y ahora realiza la verificación de identidad, la detección de vida y el monitoreo AML en una única plataforma, con señales de riesgo relacionadas con direcciones IP y números de teléfono que detectan comportamientos sospechosos desde el primer toque. Para una empresa de P2P internacionales y criptomonedas, ese es el modelo de ciclo de vida completo que funciona en producción, mucho más allá de la presentación de diapositivas.



Juan Andreu
Director de tecnología de El Dorado

"La integración de las soluciones de verificación de Sumsub ha mejorado considerablemente la seguridad y la fiabilidad de nuestra plataforma, lo que se traduce en transacciones más fluidas y una mayor tranquilidad para nuestros usuarios".



Confianza desde el primer día: monitoreo del ciclo de vida completo

La mayor parte del riesgo real surge una vez abierta la cuenta, por lo que es necesario un monitoreo continuo:

1. Las señales de comportamiento marcan las sesiones en las que se tipea, se toca y se navega de forma diferente a como lo haría un usuario real.
2. La inteligencia de dispositivo detecta que la cuenta accede desde un lugar en el que nunca antes se había conectado.
3. El monitoreo de transacciones detecta patrones que un único pago nunca revelaría, y así se descubren las redes de mulas y las capas.
4. El caso de una mula de dinero detectado semanas después de una incorporación sin incidencias lo deja claro, ya que la señal relevante nunca llegó a la primera línea de contacto.
5. La autenticación facial en momentos de alto riesgo confirma que la persona es quién dice ser.

Nada de esto afecta al usuario legítimo, y todo depende de que los datos de incorporación sigan estando activos en el sistema.

Los beneficios van más allá de la reducción de pérdidas y se extienden a la conversión: la puntuación de riesgo continua permite a los usuarios de confianza realizar su siguiente acción con menos obstáculos, y destina los escasos recursos de revisión manual a los casos que lo merecen. Una gestión basada en la confianza durante todo el ciclo de vida protege los ingresos de ambas partes, reduce las pérdidas por fraude y evita que un control generalizado ahuyente a los usuarios de buena fe debido a amenazas que, en realidad, solo representa una pequeña parte de ellos.



Lista de control de operaciones

Para los equipos que quieran convertir esto en una hoja de ruta, las prioridades son concretas:

Automatiza la validación de la identidad en el primer punto de contacto para evitar abandonos innecesarios y reserva los pasos manuales para los casos que supongan un riesgo real.

Centraliza la gestión de riesgos en un único panel para que los equipos de detección de fraude y de cumplimiento dejen de trabajar con versiones diferentes de la información.

Hace un seguimiento del abandono durante la incorporación como métrica en tiempo real y adapta el flujo en la aplicación móvil en función de lo que indiquen las cifras.

Aplica controles dinámicos y adaptados al contexto, de modo que la fricción aumente o disminuya en función del nivel de riesgo de cada usuario.

Usa señales relacionadas con el dispositivo y el comportamiento para detectar las apropiaciones de cuentas antes de que se completen, no después de que se haya transferido el dinero.

Aquí es donde la colaboración entre Certisur y Sumsub encaja en el mercado argentino.

Certisur aporta la infraestructura de confianza local en la que ya confían los bancos y las empresas argentinas: firmas electrónicas, certificados digitales, identidad digital y la reputación de un actor local consolidado dentro del sector regulado.



Néstor Markowicz
Director General de CertiSur

"Uno de los errores más frecuentes que cometen las empresas locales es dar por sentado que la identidad solo tiene que validarse una vez durante la incorporación. El verdadero riesgo operativo comienza, realmente, justo después de abrir la cuenta: las credenciales cambian, surgen nuevos vectores de amenaza y los patrones de fraude evolucionan de forma dinámica. La confianza debe gestionarse de forma activa a lo largo de todo el ciclo de vida del cliente, no solo el primer día".

Por dónde empezar

Las entidades que crecen de forma segura en Argentina consideran la verificación como una infraestructura que permanece activa durante toda la vigencia de la cuenta. En la práctica, esto se traduce en una única plataforma en la que la incorporación, la prevención del fraude y el monitoreo comparten datos, en la que las dificultades se adaptan al nivel de riesgo y en la que la confianza local se une al alcance global.

Certisur y Sumsub traen ese modelo al mercado argentino en un único lugar.

Proceso de incorporación rápido y basado en el riesgo mediante la verificación sin documentos y el chequeo de documentos. Se han impedido los casos de suplantación de identidad y las sesiones manipuladas gracias a las tecnologías de detección de vida, inteligencia de dispositivos y autenticación facial. Las redes de mulas detectadas mediante el sistema de detección de redes de fraude. La confianza se ha mantenido después del primer día gracias al monitoreo de transacciones y el manejo de casos AML, así como a la cobertura de Travel Rule para los corredores de criptomonedas que impulsan el volumen en Argentina.

Contáctenos

Hable con Sumsub

hello@sumsub.com
sumsub.com

Hable con CertiSur

atencionalcliente@certisur.com
certisur.com